日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１２月１１日

出願番号
Application Number:　特願２００２－３５９０７２

[ST.10/C]:　[ＪＰ２００２－３５９０７２]

出願人
Applicant(s):　松下電器産業株式会社

２００３年　６月２０日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０４８７２３

【書類名】　特許願

【整理番号】　2032740164

【提出日】　平成14年12月11日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　9/06

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　庄田　幸恵

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　廣田　照人

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井藤　好克

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　暗号化データ復号装置、および暗号化データ復号方法

【特許請求の範囲】

【請求項１】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、

前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持部と、

暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、

前記暗号鍵を保持する暗号鍵保持部と、

前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して、前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部と、

を有することを特徴とする暗号化データ復号装置。

【請求項２】　分割され暗号化されたプログラムをメモリ空間にコピーし、ロードした位置、ロードした分割プログラムのサイズ、プログラム識別子をアドレステーブル情報保持部に記憶させると同時に、ロードしたアドレスにすでに他の分割プログラムがロードされていた場合にはその分割プログラムの管理情報をアドレステーブル情報保持部から削除するプログラム配置位置決定部をさらに有することを特徴とする請求項１記載の暗号化データ復号装置。

【請求項３】　分割され暗号化されたプログラムをロードするためのメモリ空間の開始位置とそのサイズを指定するプログラムロード領域指定部をさらに有することを特徴とする請求項１記載の暗号化データ復号装置。

【請求項４】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持ステップと、

前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持ステップと、

暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号ステップと、

前記暗号鍵を保持する暗号鍵保持ステップと、

前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持ステップが保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して、前記メモリ配置情報保持ステップが保持するメモリ空間上の配置位置にロードする制御ステップと、

を包含することを特徴とする暗号化データ復号方法。

【請求項５】　分割され暗号化されたプログラムをメモリ空間にコピーし、ロードした位置、ロードした分割プログラムのサイズ、プログラム識別子をアドレステーブル情報保持ステップに記憶させると同時に、ロードしたアドレスにすでに他の分割プログラムがロードされていた場合にはその分割プログラムの管理情報をアドレステーブル情報保持ステップから削除するプログラム配置位置決定ステップをさらに包含することを特徴とする請求項４記載の暗号化データ復号方法。

【請求項６】　分割され暗号化されたプログラムをロードするためのメモリ空間の開始位置とそのサイズを指定するプログラムロード領域指定ステップをさらに包含することを特徴とする請求項４記載の暗号化データ復号方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、実行プログラムの逆解析や不正使用を防止する暗号化データ復号装置および暗号化データ復号方法に関する。

【０００２】

【従来の技術】

従来、暗号方式をコンピュータシステムに提供し、暗号化されたプログラムやデータを復号して利用する場合には、そのシステムの上で動作する復号プログラムを実行する。このとき、仕様が公開されたオープンなコンピュータシステムに置いては、プログラムの解析および改変が容易であるため、復号プログラムを改変することにより、もとの復号プログラムの仕様に反して、復号したデータを不正に利用することが簡単にできてしまい、システム全体の安全性は低くなるとい

う問題があった。

【０００３】

この問題を解決しようとする提案として、復号プログラム自体を暗号化し、データ復号時にのみ復号プログラムを復号して、データ復号作業を行う手段を採用し、これにより、復号プログラムの解析および改変を困難にするものが知られている（例えば、特許文献１参照）。しかし、復号プログラムを復号するプログラムの解析、および改竄が成功すると、改竄プログラムの実行を防ぐことはできない。これに対し、復号プログラムの正当性を暗号化データの復号時に認証できるようにし、改竄された復号プログラムによる意図しない目的への復号したデータの流用を防止する提案がある（例えば、特許文献２参照）。

【０００４】

ところが、正当性が証明された復号プログラムを実行する場合には、コンピュータシステム上のメモリに復号された状態でプログラムがロードされる。このときに、不正な割り込み等により処理の流れを横取りされると、全てのプログラムが覗き見されてしまう。

【０００５】

また、メモリ上へのプログラムのロード方法として、オーバレイリンカ／ローダが知られている（例えば、非特許文献１参照）。オーバレイは、プログラムサイズよりも小さいメモリにプログラムを収めるために使われる手法である。プログラムのコードを小さなサイズでセグメント分割する。オーバレイのいくつかのセグメントは、同じメモリを共有する。プログラムが起動するとき、システムは、プログラムのエントリポイントを持つセグメントをロードする。オーバレイローダは、呼び出し先へのパスが含まれる各セグメントを、必要に応じて随時、ロードする。

【０００６】

しかし、従来のオーバレイリンカ／ローダでは、必要なセグメントを必要な時に順に限られた大きさのメモリ上にロードし、要らなくなったときに削除、または、他のプログラムが上書きすることによって消去されるため、メモリ上にプログラムのコードやデータが残されたままの状態になってしまうという問題があっ

た。また、オーバレイローダがプログラムをロードするアドレスが固定されるため、プログラムへのアクセスが容易に解読できてしまうという問題があった。

【０００７】

以上のように、従来の技術では、一般的なコンピュータシステムにおいては、復号プログラムがメモリ上にロードされているときに不正な割り込みが発生した場合、全てのプログラムが覗き見されてしまい、復号プログラムのアルゴリズムや暗号鍵が暴露されてしまう。また、近年のコンピュータシステムは、メモリに制約を持たないのでオーバレイの手法を用いることはほとんどなく、プログラム全体をメモリ上に展開している。このため、システム全体の安全性が低くなってしまうという問題がある。

【０００８】

【特許文献１】

特開平９－６２３２号公報

【特許文献２】

特開平１１－３９１５６号公報

【非特許文献１】

Ｌｉｎｋｅｒｓ＆Ｌｏａｄｅｒｓ、Ｊｏｈｎ　Ｒ．Ｌｅｖｉｎｅ、オーム社、ｐ１６５

【０００９】

【発明が解決しようとする課題】

本発明は、仕様が公開されているオープンなコンピュータシステムにおいても、プログラムを部分的に復号しながらメモリ上にロードできるようにすることにより、不正な割り込み等で処理の流れが横取りされても、メモリ上からプログラムの全体の覗き見を防止することを目的としている。

【００１０】

【課題を解決するための手段】

この課題を解決するために、本発明は、単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、前記プログラムの記憶装置上の位置情報を保持するアドレ

ステーブル情報保持部と、暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、前記暗号鍵を保持する暗号鍵保持部と、前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部とを備えたものである。

【００１１】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて説明する。

【００１２】

（実施の形態１）

図１は、本発明の暗号化データ復号装置の構成を示す機能ブロック図である。図１においてメモリ配置情報保持部１０４は単位毎に分割されたプログラムを実行する際にメモリ空間上の配置位置を示す情報を保持し、アドレステーブル情報保持部１０３は、分割されたプログラムがメモリ上のどの位置に格納されているかという情報を暗号化して保持している。また暗号化データ復号部１０２は、暗号化されたデータを暗号鍵に基づき復号し、暗号鍵保持部１０１は暗号化データ復号部１０２が暗号化データを復号化する際に用いる暗号鍵を保持し、またアドレス情報認証部１０５は、アドレステーブル情報保持部１０３が保持する情報が正当なものか否かを認証し、メモリアドレス定義部１０８はメモリ配置情報保持部１０４の保持するメモリ空間上の配置位置をプログラム生成時にあらかじめ定義する。

【００１３】

プログラム生成部１１１はメモリアドレス定義部１０８が定義した情報に基づいて単位毎に分割され暗号化されたプログラムを生成する。暗号化情報復号部１０９は、暗号化されたメモリ配置情報保持部１０４の配置情報を暗号鍵に基づき復号する。暗号化テーブル情報復号部１１０は暗号化されたアドレステーブル情報保持部１０３の位置情報を暗号鍵に基づき復号する。不正アクセス防止部１０７は、プログラム実行中に割り込み等により不正に処理の流れを奪われた場合に

、それを検知し対抗措置をとる。さらに復号支援プログラム認証部１００は暗号化データ復号部１０２が暗号化されたデータを復号する際に用いる復号支援プログラムが正当なものか否かを認証する。制御部１０６は、暗号化データ復号部１０２に復号指示を出し、アドレステーブル情報保持部１０３が保持する情報に従ってメモリ配置情報保持部１０４が保持するメモリ空間上の配置位置に従って単位毎にコンピュータシステムのメモリ空間上にプログラムを配置しながら実行する。

【００１４】

図２は、制御部１０６が配置するメモリ配置構成の概念図である。

【００１５】

図３は、メモリ配置情報保持部１０４が保持する暗号化されたアドレス情報および復号化されたアドレス情報およびハードディスク上のイメージ図である。

【００１６】

図４は、メモリ配置情報保持部１０４が保持するメモリ空間上の配置位置を示す情報の概念図である。

【００１７】

上記のような構成の暗号化データ復号装置において単位毎に分割されたプログラムのロード処理の具体的な流れを図５を用いて説明する。

【００１８】

ここでいうプログラムのロードとは、プログラムを実行できるようにハードディスクのような２次記憶装置からメインメモリにコピーすることである。また単位毎に分割されたプログラムとは、１つのソースファイルまたは関連するソースファイルのグループから生成されたオブジェクトコードを指している。このオブジェクトコードとは具体的には一つのプログラムを構成する一部分を示すサブプログラムであったりあるいはライブラリモジュールそのものを指している。

【００１９】

＜プログラムのロード手順＞

１．制御部１０６は、暗号化テーブル情報復号部１１０に対してデータを復号化するよう指示を出し（Ｓ５０１）、続いてロードすべきプログラムＡが格納さ

れているアドレスの情報を取得するためにアドレステーブル情報保持部１０３の情報を読み出す（Ｓ５０２）。

【００２０】

２．暗号化テーブル情報復号部１１０は、制御部１０６から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する（Ｓ５０３）。この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【００２１】

３．２．で認証に成功した場合、暗号化テーブル情報復号部１１０は、図３の（３－１）に示すようなデータを暗号鍵保持部１０１が保持している暗号化されたデータを復号するための鍵に基づき読み出したデータを復号し（Ｓ５０４）、プログラムＡが格納されている図３の（３－２）に示すようなアドレスの情報を得る。もし２．で認証に失敗した場合、暗号化テーブル情報復号部１１０はデータの復号を行わずプログラムの処理を中断し（Ｓ５１７）、制御部１０６は、メモリ空間上に復号されたデータがロードされている場合は消去する（Ｓ５１８）。

【００２２】

４．続いてアドレス情報認証部１０５は、３．で得たアドレス情報が正当なものであるか否かを認証する（Ｓ５０５）。この認証には、２．の認証処理で用いたものと同じ一方向ハッシュ関数等、一般に用いられている認証技術を用いる。アドレス情報認証部１０５がアドレス情報が正当なものであると認証した場合に、ステップ５．に進み、認証に失敗した場合は、制御部１０６はプログラムの処理を中断し（Ｓ５１７）、メモリ空間上にデータがロードされている場合は消去する（Ｓ５１８）。

【００２３】

５．引き続き制御部１０６は、暗号化データ復号部１０２に指示を出す（Ｓ５０６）。

【００２４】

６．暗号化データ復号部１０２は、制御部１０６から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する（Ｓ５０７）。この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【００２５】

７．６．で認証に成功した場合、図３の（３－３）に示すようなハードディスクの該当のアドレス位置から読み出したプログラムＡを読み出す（Ｓ５０８）。暗号化データ復号部１０２は読み出された暗号化されたプログラムＡを復号する（Ｓ５０９）。６．で認証に失敗した場合、データの復号を行わずプログラムの処理を中断し（Ｓ５１７）、制御部１０６は、メモリ空間上に復号されたデータやプログラムがロードされている場合は消去する（Ｓ５１８）。

【００２６】

８．さらに制御部１０６は、暗号化情報復号部１０９に復号指示を出す（Ｓ５１０）。

【００２７】

９．暗号化情報復号部１０９は、制御部１０６から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する（Ｓ５１１）。この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【００２８】

１０．９．で認証に成功した場合、暗号化情報復号部１０９はメモリ配置情報保持部１０４が保持する図４に示すようなメモリ空間上の配置位置情報の情報を読み出し（Ｓ５１３）、読み出されたメモリ空間上の配置位置情報を復号化し（Ｓ５１４）、復号化された配置位置情報に従ってプログラムＡを予め定められた

メモリ空間上のＯＳ１－１というメモリ空間にロードする（Ｓ５１５）。９．で認証に失敗した場合、配置情報の復号化は行わずに、プログラムの処理を中断し（Ｓ５１７）、制御部１０６は、メモリ空間上に復号されたデータがロードされている場合は消去する（Ｓ５１８）。

【００２９】

１１．制御部１０６は、プログラムＡが呼び出す順に分割されたプログラムＢ～プログラムＩを１．～１０．の手順を繰り返すことによりロードする。

【００３０】

上記に述べたステップの暗号鍵保持部１０１は、具体的には例えばＤＥＳのような暗号化方式に用いる暗号鍵を持ち、通常、プログラムの一定領域に埋め込まれるかあるいはユーザには見えない部分あるいはファイルに秘匿されている。もちろん、暗号方式はこれ以外のものでもよい。簡易化する方法として、単に値の排他的論理和を取る方法等でもよい。また秘匿の方法もこれに限るものではない。

【００３１】

また、暗号化データ復号部１０２、暗号化テーブル情報復号部１１０、暗号化情報復号部１０９は同じものであっても構わないし、異なるものであってもよい。

【００３２】

なお、上記のステップに従ってプログラムをロードし、プログラムを実行した後メモリ空間上に展開されたプログラムは、実行直後に消去してもよいし、または次のプログラムがロードされる際に上書きすることによって消去するようにしてもよい。このようなプログラムを消去するタイミングは、そのプログラムの重要性やパフォーマンスによってプログラム生成時にユーザが別途指定するようにしてもよい。

【００３３】

次に、実施の形態２について述べる。

【００３４】

（実施の形態２）

実施の形態１のメモリ配置情報保持部１０４は、プログラム生成時に決定された固定されたメモリ配置情報を保持しているため、上記プログラム実行時に各分割されたプログラムは毎回同じ配置位置にロードされる。この毎回同じ配置位置をハッカーによって見破られることを避けるために、プログラムロード領域指定部１１２によって、各分割プログラムをロードするメモリ領域を毎回変化させる。また、プログラム配置位置決定部１１３によって、このメモリ配置情報保持部１０４に保持するメモリ配置情報を毎回変化させる。

【００３５】

図６はメモリ配置情報保持部１０４が保持するメモリ配置情報の図である。

【００３６】

プログラム配置位置決定部１１３が決定するメモリ空間上の配置位置情報は、図４に示すようなメモリ配置位置情報および図６の（１）～（３）に示されるようにプログラムがロードされる度にアドレス情報が入れ替わる。

【００３７】

実施の形態２の動作の流れを実施の形態１の＜プログラムのロード手順＞を用いて説明する。＜プログラムのロード手順＞１．～９．までは実施の形態１と同様である。

【００３８】

実施の形態１の＜プログラムのロード手順＞の１０．以降の代わりに以下のような手順で動作する。

【００３９】

１０．プログラムロード領域指定部１１２は、分割プログラムをロードするメモリ領域の開始アドレスとサイズを指定し、メモリ配置情報保持部１０４が記憶する。

【００４０】

１１．９．で認証に成功した場合、プログラムＡを１０．で指定したプログラムロード領域内にロードする。このときのロード位置は、プログラム配置位置決定部１１３によって決定される。

【００４１】

１２．９．で認証に失敗した場合、配置情報の復号化は行わずに、プログラムの処理を中断し（Ｓ５１７）、制御部１０６は、メモリ空間上に復号されたデータがロードされている場合は消去する（Ｓ５１８）。

【００４２】

１３．制御部１０６は、プログラムＡが呼び出す順に分割されたプログラムＢ～プログラムＩを１．～１２．の手順を繰り返すことによりロードし、実行する。

【００４３】

図７は、プログラム配置位置決定部１１３における配置位置決定の流れを示すフローチャートである。

【００４４】

１１－１．アドレステーブル情報保持部１０３で保持している分割プログラムのロード領域の管理情報と、ロードされている分割プログラムの管理情報と、ロードしようとしている分割プログラムのサイズを比較して、十分な空き領域があるかどうか調べる（Ｓ７０１）。十分な空き領域があれば、１１－２．の処理に進む。なければ、１１－３．の処理に進む。

【００４５】

１１－２．空き領域に分割プログラムをロードする（Ｓ７０２）。１１－５．に進む。

【００４６】

１１－３．アドレステーブル情報保持部１０３から、ロードされている分割プログラムのうち、最も古くからロードされているものを求め、それを削除する（Ｓ７０４）。１１－４．に進む。

【００４７】

１１－４．削除された分割プログラムの管理情報をアドレステーブル情報保持部１０３から削除する（Ｓ７０５）。１１－１．に戻る。

【００４８】

１１－５．ロードした分割プログラムの開始位置、サイズ、プログラム識別子をアドレステーブル情報保持部１０３に図６のように記憶させる（Ｓ７０３）。

終了する。

【００４９】

このようにプログラム配置位置決定部１１３は、メモリ配置情報保持部１０４が保持する予め定められたアドレスの代わりに、プログラムが実行される度に分割プログラムの配置位置を決定することにより、分割されたプログラムが毎回同じアドレスにロードされないようにすることが可能になる。

【００５０】

なお、１１－３．において、次にロードする位置を最も古くからロードされているものの上にロードする代わりに、ランダムに位置を決定することにより、各分割プログラムの先頭アドレスをずらして、毎回同じアドレスにロードされないようにするとしてもよい。

【００５１】

また、１１－３．および１１－４．において、最も古い分割プログラムを削除し、十分な空き領域が得られるまで１１－１．から繰り返すとしたが、繰り返しを行わず、最も古い分割プログラムの先頭から連続した領域に新しい分割プログラムをロードしてもよい。このとき、２つ以上の分割プログラムが１度に削除されることもある。

【００５２】

以上のように動作するプログラムを生成するプログラム生成部１１１の動作について述べる。

【００５３】

通常、ソースコードやライブラリの集合から実行形式のプログラムを生成する際には、コンパイラを用いてソースコードをオブジェクトコードに変換する。さらに、リンカを用いて、これらのオブジェクトコードや標準のライブラリを組み合わせて、実行形式のプログラムが生成される。

【００５４】

本実施の形態のプログラム生成部１１１は、プログラムを市販のコンパイラでコンパイルした結果得られるオブジェクトファイルに対して、オーバレイロードを行うために必要な情報を追加してオブジェクトファイルを変形する。さらに、

市販のリンカを用いて、これらの変形したオブジェクトファイル、ローダ機能を実現するライブラリ、標準のライブラリから実行形式のプログラムを生成する。プログラム生成部１１１に市販のコンパイラやリンカの機能を組み込んでもよい。

【００５５】

【発明の効果】

以上、説明したように本発明は、分割プログラムをロードする際のメモリ領域を毎回指定可能として、ロードする領域のメモリ位置を毎回変えることにより、命令コードがロードされるアドレスが変えることができる。また、分割プログラムロード時にロードする開始位置を毎回決定することを可能とすることにより、命令コードがロードされるアドレスが変えることができる。これらの結果、プログラムの動作を解析することが困難になり、安全性の高い耐タンパ化プログラムが提供できる。

【図面の簡単な説明】

【図１】

暗号化データ復号装置の構成を示す機能ブロック図

【図２】

制御部が配置するメモリ配置構成の概念図

【図３】

メモリ配置情報保持部が保持する暗号化されたアドレス情報および復号化されたアドレス情報およびハードディスク上のイメージ図

【図４】

メモリ配置情報保持部が保持するメモリ空間上の配置位置を示す概念図

【図５】

ロード処理を表すフローチャート

【図６】

メモリ配置情報保持部が保持するメモリ配置情報の図

【図７】

プログラム配置位置決定部における配置位置決定の流れを示すフローチャート

【符号の説明】

１００　復号支援プログラム認証部

１０１　暗号鍵保持部

１０２　暗号化データ復号部

１０３　アドレステーブル情報保持部

１０４　メモリ配置情報保持部

１０５　アドレス情報認証部

１０６　制御部

１０７　不正アクセス防止部

１０８　メモリアドレス定義部

１０９　暗号化情報復号部

１１０　暗号化テーブル情報復号部

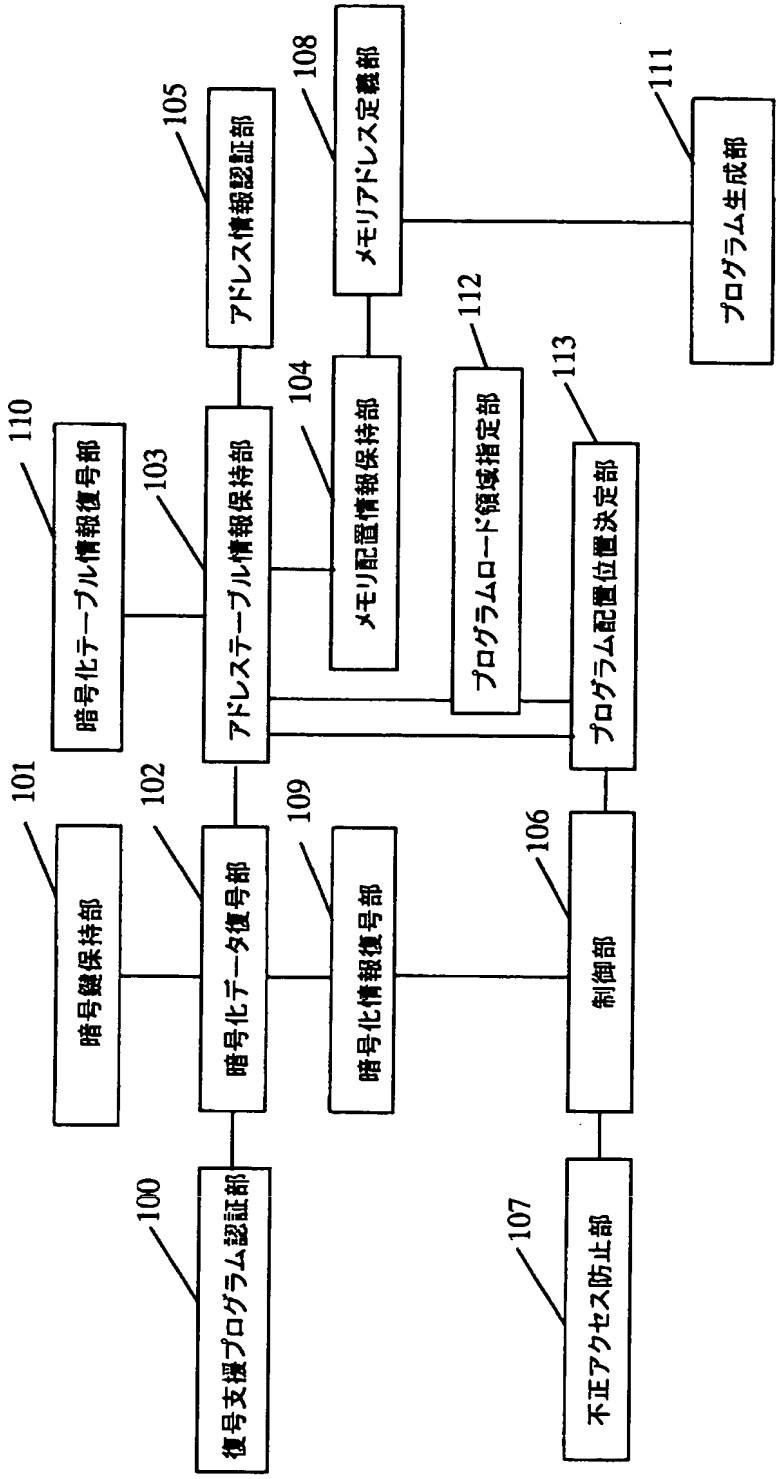
１１１　プログラム生成部

１１２　プログラムロード領域指定部

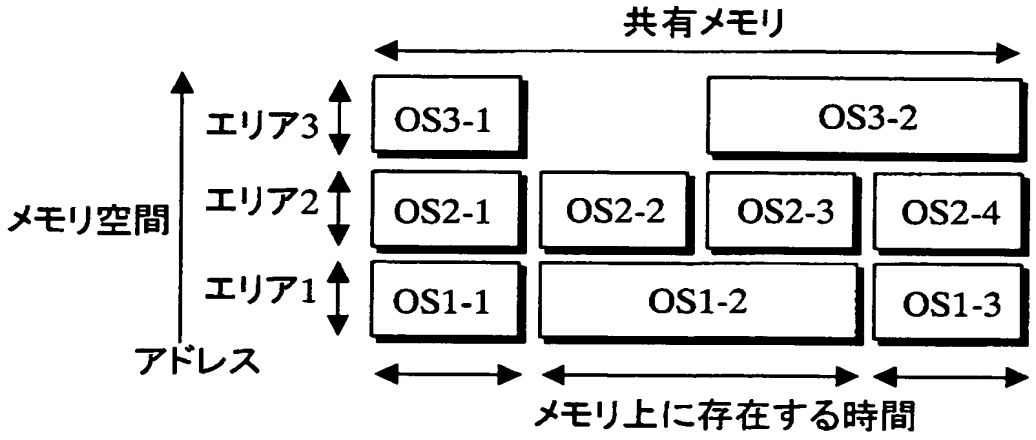
１１３　プログラム配置位置決定部

【書類名】　　図面

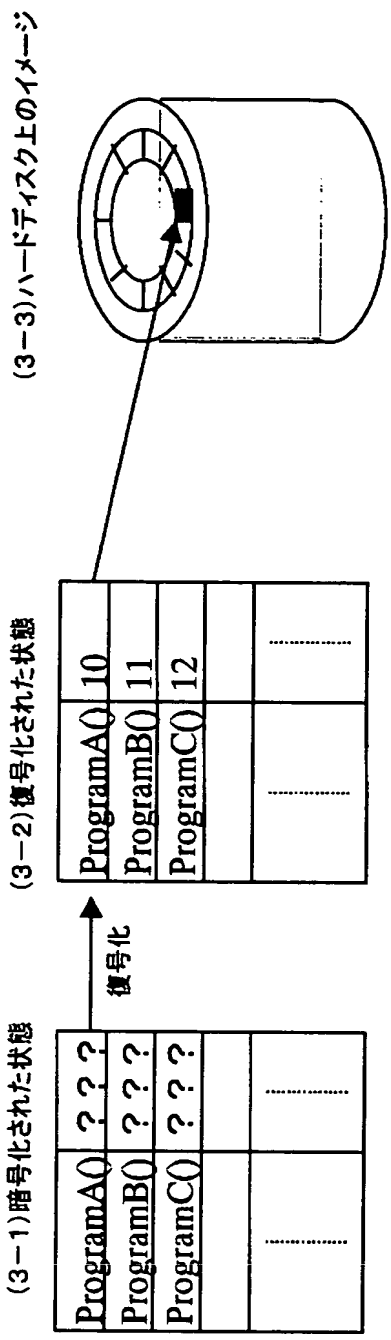
【図１】


復号支援プログラム認証部
100
暗号鍵保持部
101
暗号化データ復号部
102
暗号化情報復号部
109
制御部
106
不正アクセス防止部
107
暗号化テーブル情報復号部
110
アドレステーブル情報保持部
103
メモリ配置情報保持部
104
プログラムロード領域指定部
112
プログラム配置位置決定部
113
アドレス情報認証部
105
メモリアドレス定義部
108
プログラム生成部
111

【図２】


共有メモリ
エリア3
エリア2
エリア1
メモリ空間
アドレス
OS3-1
OS3-2
OS2-1
OS2-2
OS2-3
OS2-4
OS1-1
OS1-2
OS1-3
メモリ上に存在する時間

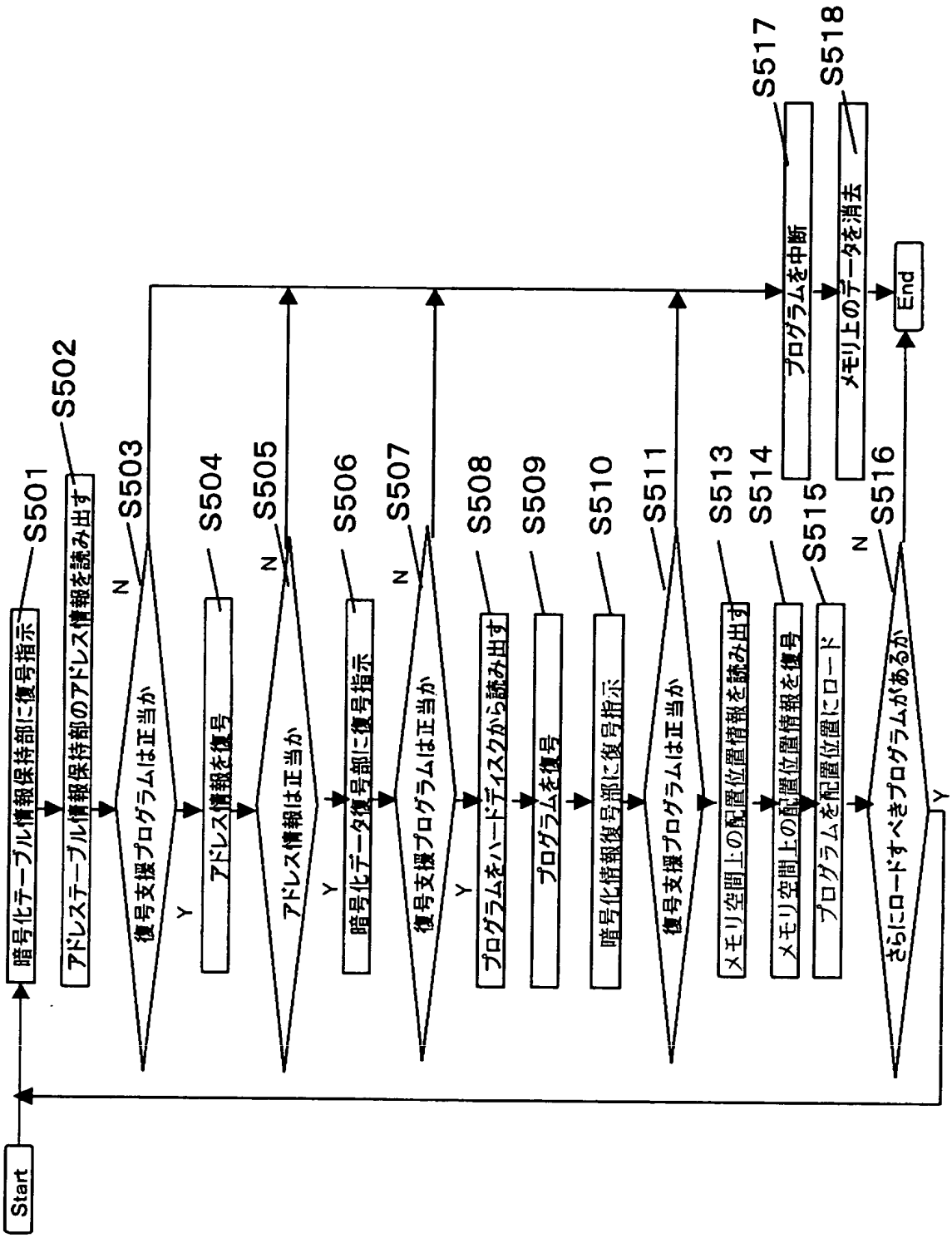
【図３】


(3－3)ハードディスク上のイメージ
(3－2)復号化された状態
ProgramA() 10
ProgramB() 11
ProgramC() 12
復号化
(3－1)暗号化された状態
ProgramA() ???
ProgramB() ???
ProgramC() ???

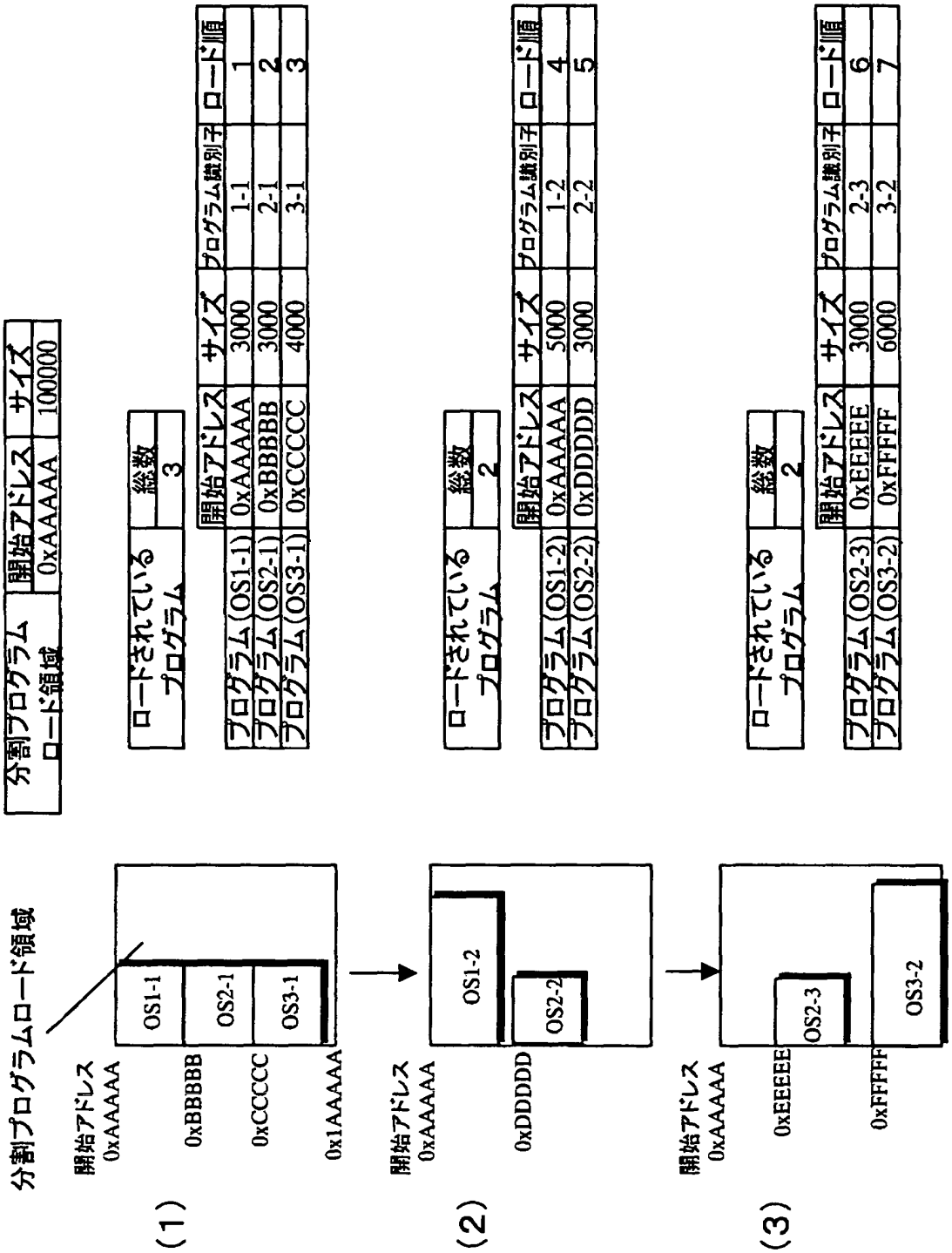
【図４】

#Load data エリア１－３	
エリア１	Program A= OS1-1
	Program B= OS1-2
	Program C= OS1-3
エリア２	Program D= OS2-1
	Program E= OS2-2
	Program F= OS2-3
エリア３	Program G= OS3-1
	Program H= OS3-2
	Program I = OS3-3

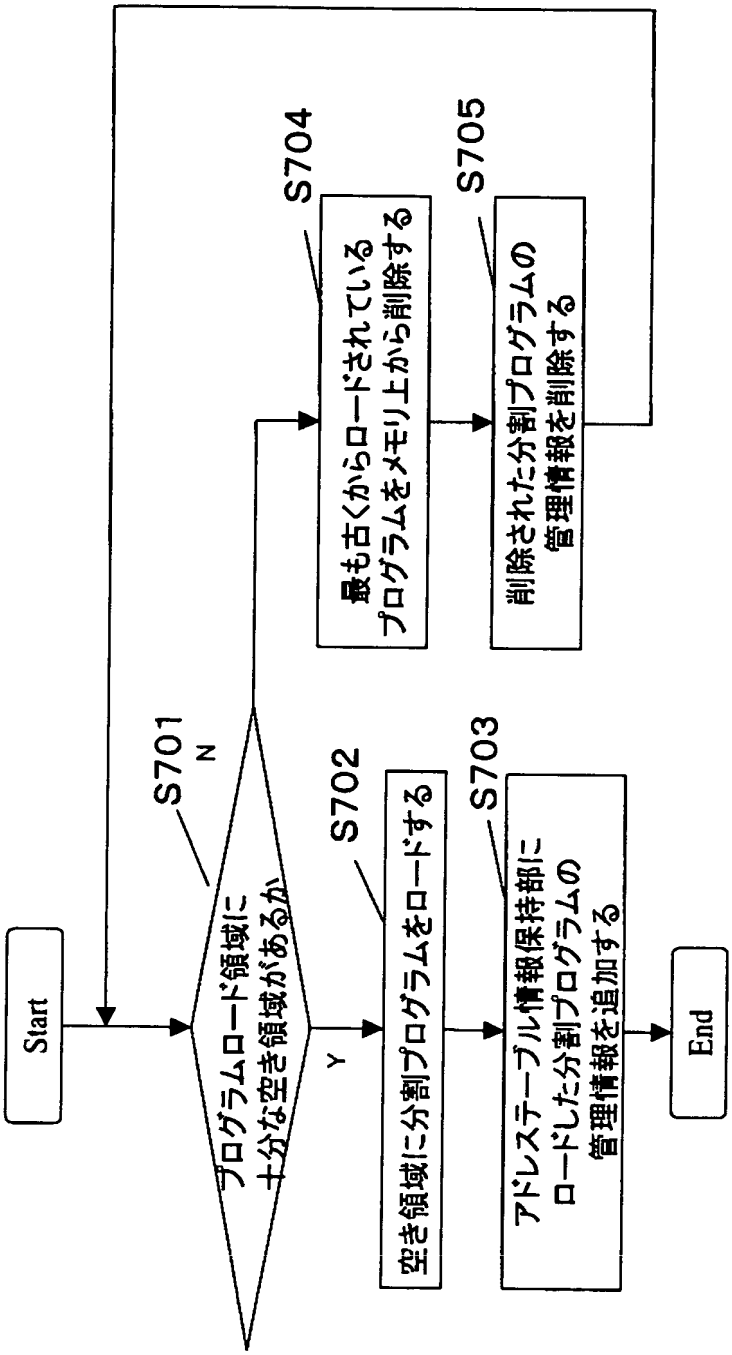
【図５】


Start
暗号化テーブル情報保持部に復号指示
S501
アドレステーブル情報保持部のアドレス情報を読み出す
S502
復号支援プログラムは正当か
S503
N
Y
アドレス情報を復号
S504
アドレス情報は正当か
S505
N
Y
暗号化データ復号部に復号指示
S506
復号支援プログラムは正当か
S507
N
Y
プログラムをハードディスクから読み出す
S508
プログラムを復号
S509
暗号化情報復号部に復号指示
S510
復号支援プログラムは正当か
S511
N
Y
メモリ空間上の配置位置情報を読み出す
S513
メモリ空間上の配置位置情報を復号
S514
プログラムを配置位置にロード
S515
さらにロードすべきプログラムがあるか
S516
N
Y
プログラムを中断
S517
メモリ上のデータを消去
S518
End

【図６】


分割プログラム
ロード領域
開始アドレス
0xAAAAA
サイズ
100000
ロードされている
プログラム
総数
3
開始アドレス
サイズ
プログラム識別子
ロード順
プログラム(OS1-1)
0xAAAAA
3000
1-1
1
プログラム(OS2-1)
0xBBBBB
3000
2-1
2
プログラム(OS3-1)
0xCCCCC
4000
3-1
3
ロードされている
プログラム
総数
2
開始アドレス
サイズ
プログラム識別子
ロード順
プログラム(OS1-2)
0xAAAAA
5000
1-2
4
プログラム(OS2-2)
0xDDDDD
3000
2-2
5
ロードされている
プログラム
総数
2
開始アドレス
サイズ
プログラム識別子
ロード順
プログラム(OS2-3)
0xEEEEE
3000
2-3
6
プログラム(OS3-2)
0xFFFFF
6000
3-2
7
分割プログラムロード領域
開始アドレス
0xAAAAA
OS1-1
OS2-1
OS3-1
0xBBBBB
0xCCCCC
0x1AAAAA
(1)
開始アドレス
0xAAAAA
OS1-2
OS2-2
0xDDDDD
(2)
開始アドレス
0xAAAAA
0xEEEEE
OS2-3
OS3-2
0xFFFFF
(3)

【図７】


Start
S701
プログラムロード領域に
十分な空き領域があるか
N
Y
S702
空き領域に分割プログラムをロードする
S703
アドレステーブル情報保持部に
ロードした分割プログラムの
管理情報を追加する
End
S704
最も古くからロードされている
プログラムをメモリ上から削除する
S705
削除された分割プログラムの
管理情報を削除する

【書類名】　要約書

【要約】

【課題】　分割プログラムをロードする領域のメモリ位置を毎回変えることにより、命令コードがロードされるアドレスを変えることができる耐タンパ化プログラムを提供する。

【解決手段】　単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、プログラムの２次記憶装置上の位置情報を保持するアドレステーブル情報保持部と、分割され暗号化されたプログラムをメモリ空間にコピーし、ロードした位置、ロードしたプログラムのサイズ、識別子をアドレステーブル情報保持部に記憶させると同時に、すでに他のプログラムがロードされていた場合にはそのプログラムの管理情報をアドレステーブル情報保持部から削除するプログラム配置位置決定部とを有する。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社